TLP:CLEAR

Prehľad bezpečnostných udalostí csirt.upjs.sk 10.2.2025 – 16.2.2025

Google opravil chybu odhaľujúcu e-mailové adresy používateľov YouTube

Spoločnosť Google opravila dve zraniteľnosti, ktoré v kombinácii mohli odhaliť e-mailové adresy používateľov YouTube, čo predstavovalo vážne riziko pre anonymitu tvorcov obsahu, whistleblowerov a aktivistov. Tieto chyby objavili bezpečnostní výskumníci Brutecat a Nathan, ktorí zistili, že prostredníctvom YouTube a Pixel Recorder API je možné získať interné identifikátory používateľov, známe ako Gaia ID, a následne ich previesť na e-mailové adresy. Prvá zraniteľnosť spočívala v tom, že pri pokuse o blokovanie používateľa v živom chate YouTube sa v odpovedi API zobrazilo obfuskované Gaia ID cieľového používateľa. Druhá zraniteľnosť umožňovala pomocou Pixel Recorder API previesť získané Gaia ID na e-mailovú adresu.

Apple opravuje zero-day zraniteľnosť zneužívanú v "mimoriadne sofistikovaných" útokoch

Spoločnosť Apple vydala bezpečnostné aktualizácie, ktoré riešia zero-day zraniteľnosť CVE-2025-24200. Táto chyba umožňovala fyzickým útočníkom deaktivovať USB Restricted Mode na uzamknutých zariadeniach, čo mohlo viesť k neoprávnenému prístupu k dátam. USB Restricted Mode, predstavený v iOS 11.4.1, blokuje dátové pripojenia cez USB, ak je zariadenie uzamknuté viac ako hodinu, čím chráni pred forenznými nástrojmi, ako sú GrayKey a Cellebrite. Apple uviedol, že táto zraniteľnosť bola zneužitá v "mimoriadne sofistikovaných" útokoch zameraných na konkrétne osoby.

Hackeri zneužívajú CAPTCHA trik na Webflow CDN PDF súboroch na obídenie bezpečnostných skenerov

V nedávnej phishingovej kampani útočníci využívajú falošné PDF dokumenty hostované na Webflow Content Delivery Network (CDN) s cieľom odcudziť informácie o kreditných kartách a spôsobiť finančné podvody. Tieto PDF súbory obsahujú obrázok napodobňujúci CAPTCHA výzvu, po kliknutí naň sú obete presmerované na phishingovú stránku s reálnou CAPTCHA od Cloudflare Turnstile, čo zvyšuje dôveryhodnosť útoku a pomáha obísť detekciu statickými skenermi. Po vyriešení CAPTCHA sú používatelia vyzvaní na zadanie osobných a finančných údajov. Táto aktivita prebieha od druhej polovice roku 2024 a zameriava sa na používateľov hľadajúcich dokumenty cez vyhľadávače ako Google.

Google Chrome zavádza AI-poháňanú bezpečnostnú funkciu

Google rozšíril Enhanced protection v prehliadači Chrome o umelú inteligenciu (AI), ktorá poskytuje ochranu v reálnom čase proti škodlivým webom, sťahovaniam a rozšíreniam. AI analyzuje vzorce hrozieb skôr, než sú identifikované v databázach, čím zlepšuje prevenciu proti phishingu a malware útokom. Táto funkcia je voliteľná, predvolene vypnutá, a používatelia ju môžu aktivovať v nastaveniach Chrome na Windows, Android a iOS.

Ruskí hackeri zneužívajú 'device code phishing' na prevzatie účtov

Spoločnosť Microsoft upozorňuje na novú hrozbu označovanú ako Storm-2372, ktorá od augusta 2024 cieli na rôzne sektory vrátane vládnych organizácií, IT služieb, obrany a energetiky. Útočníci, pravdepodobne napojení na ruské záujmy, sa vydávajú za významné osoby na platformách ako WhatsApp, Signal a Microsoft Teams, aby získali dôveru obetí. Používajú techniku nazývanú 'device code phishing', kde obete presvedčia, aby zadali špeciálny kód na legitímnej prihlasovacej stránke, čím útočníkom umožnia získať autentifikačné tokeny a prístup k ich účtom. Tieto tokeny potom slúžia na prístup k ďalším službám, ako je e-mail alebo cloudové úložisko, bez potreby hesla.